University of Bristol
Information Security Policy

Title:	**Information Handling**
Reference:	**ISP-07**
Status:	**Approved**
Version:	**1.5**
Date:	**July 2013**
Reviewed:	**February 2019**
Classification:	**Public**

Contents

Introduction

This Information Handling Policy is a sub-policy of the Information Security Policy (ISP-01) and sets out the requirements relating to the handling of the University's information assets. Information assets must be managed in order to protect against the consequences of breaches of confidentiality, loss of integrity, interruption to availability, and non-compliance with legislation which would otherwise occur.

Inventory and ownership of information assets

An inventory of the University's main information assets will be developed and maintained and the ownership of each asset clearly stated.

Each asset will have a nominated owner who will be assigned responsibility for defining the appropriate uses of the asset and ensuring that appropriate security measures are in place to protect the asset.

Security classification

Each information asset will be assigned a security classification by the asset owner which reflects the sensitivity of the asset according to the following classification scheme:

- Public – available to any member of the public without restriction.
- Open – available to any authenticated member of the University.
- Confidential – available only to specified members, with appropriate authorisation.
- Sensitive and Confidential – available to only a very small number of members, with appropriate authorisation.
- Secret – the most restricted category. It is not anticipated that many University assets will be assigned this classification.

Any information which is disclosable under the Freedom of Information Act 2000 will be classified as public. Any data which is classified as sensitive personal data under the Data Protection Act 2018 (or its successor legislation) will be classified as strictly confidential. Any data which is subject to the Official Secrets Act 1989 will be classified as secret. Any information which is not explicitly classified will be classified as open, by default.

Access to information

Members of the University will be granted access to the information they need in order to fulfill their roles within the University. Members who have been granted access must not pass on information to others unless the others have also been granted access through appropriate authorisation.

Disposal of information

Great care needs to be taken to ensure that information assets are disposed of securely.

Confidential paper waste must be disposed of in accordance with formal University procedures (which are documented on the University's Sustainability website).

Electronic information must be securely erased or otherwise rendered inaccessible prior to leaving the possession of the University, unless the disposal is undertaken under contract by an approved contractor.

In cases where a storage system (for example a computer disc) is required to be returned to a supplier it should be securely erased before being returned unless contractual arrangements are in place with the supplier which guarantee the secure handling of the returned equipment. If this is not possible, then the storage system should not be returned to the supplier and should remain in the possession of the University until it is disposed of securely.

Removal of information

University data which is subject to the Data Protection Act or which has a classification of confidential or above must be stored using University facilities or with third parties subject to a formal, written legal contract with the University. In cases where it is necessary to otherwise remove data from the University, appropriate security measures must be taken to protect the data from unauthorised disclosure or loss. Information classed as confidential or above in electronic form must be strongly encrypted prior to removal. Secret data must never be removed except with the explicit written permission of the data owner.

Particular care needs to be taken when information assets are in transit. University supplied mobile devices must always be fully encrypted.

Using personally owned devices

Any processing or storage of University information using personally owned devices must be in compliance with the University's Mobile and Remote Working Policy (ISP-14).

Information on desks, screens and printers

Members of staff who handle confidential paper documents should take appropriate measures to protect against unauthorised disclosure, particularly when they are away from their desks. Confidential documents should be locked away overnight, at weekends and at other unattended times.

Care should also be taken when printing confidential documents to prevent unauthorised disclosure.

Computer screens on which confidential or sensitive information is processed or viewed should be sited in such a way that they cannot be viewed by unauthorised persons and all computers should be locked while unattended.

Backups

Information owners must ensure that appropriate backup and system recovery measures are in place. Where backups are stored off site, appropriate security

measures must be taken to protect against unauthorised disclosure or loss. Recovery procedures should be tested on a regular basis.

Information which is entrusted to the care of IT Services will meet these requirements.

Exchanges of information

Whenever significant amounts of personal data or other confidential information are exchanged with other organisations, appropriate information security measures must be established to ensure the integrity and confidentiality of the data transferred. Regular exchanges must be covered by a formal written agreement with the third party.

Information classified as sensitive and confidential may only be exchanged electronically both within the University and in exchanges with third parties if the information is strongly encrypted prior to exchange. Information classified as secret may not be transmitted electronically except with the explicit written permission of the information owner.

When exchanging information by email or fax, recipient addresses should be checked carefully prior to transmission.

Unsolicited emails, faxes, telephone calls, instant messages or any other communication requesting information which is not classified as public should not be acted upon until and unless the authenticity and validity of the communication has been verified.

Members of the University must not disclose nor copy any information classified as confidential or above unless they are authorised to do so.

Reporting losses

All members of the University have a duty to report the loss, suspected loss or unauthorised disclosure of any University information asset to the information security incident response team (cert@bristol.ac.uk).

References and further guidance

Mobile and Remote Working Policy (ISP-14):

http://www.bris.ac.uk/infosec/policies/docs/isp-14.pdf